between said first computer device and said second computer device.

33. [new] The method of claim 30 wherein the step of determining what, if any, port translations are occurring in communications between said first computer device and said second computer device is accomplished by comparing the port number in a packet header for a packet of a protocol that can withstand port translations and which encapsulates an IKE protocol packet sent from said second computer device to said first computer device, and if said port number is not a port number associated with the IKE protocol, concluding that one or more port translations is occurring on a data path between said second computer device and said first computer device.

REMARKS

Claims 1-23 were rejected as anticipated by the Nessett patent, 6,055,236. An anticipation rejection is only proper when all the elements of the claimed invention are found in a single reference, united or arranged in the same way as in the claim. Donner, *Patent Prosecution*, Chapter 6 on Anticipation, p. 323 (BNA Book 1996).

In the Nessett reference, there is no teaching of the first step of claim 1, *i.e.*, determining what if any network address translations and/or protocol conversions are occurring in the data path between the first computer device and the second computer device. Nessett's entire disclosure is dedicated to teaching how distributed network address translation using the PAP protocol can be done both with and without security (IPSEC). Nessett assumes as his starting position that there are multiple devices on a local area network behind a router and that the router is coupled to other networks. The devices on the local area network do not have globally unique IP addresses - only the edge router of the first network has such a globally unique IP address. Therefore,

Nessett assumes the NAT is occurring at the edge router and that this is the problem he is attempting to solve because NAT is incompatible with IPsec thereby precluding the devices on the LAN from using IPsec. Col. 25, lines 54 -67 and Col. 26, lines 1 -7.

The solution Nessett teaches is to substitute distributed NAT for NAT by using the PAP protocol to allow devices on the LAN to obtain a unique port number which, when combined with the globally unique IP address of the edge router, makes a unique security name space or identity to which a public key may be bound for purposes of practicing IPsec. Col. 25, lines 54 -67 and Col. 26, lines 1 -7. To allow secure communications between the devices on the local area network and devices on other networks, the PAP protocol is used to request unique port numbers from the edge router. Each process or device which needs to communicate obtains a unique port number and that port number is put in a field in the TCP header with the router's globally unique IP address in the IP packet header. The combination of the unique port number and the unique IP address is used by the edge router to route packets from a device on the LAN to other devices on other networks, without network address translation, *i.e.,* no translations of source or destination IP addresses actually occur in the edge router since the unique port number and the globally unique IP address of the edge router are all that are needed in the edge router's routing tables to get packets where they need to go. Col. 16, Lines 43 to 65.

Security protocols in Nessett are implemented by confining security processing completely within the IP layer with all DNAT processing running above the IP layer to avoid violating IP security parameters (encapsulation). Col. 21, lines 4-8. IPsec protocol headers such as AH or ESP headers are put in the protocol field 216 of the IP header as shown in Figure 15. These headers contain an numerical value called an SPI which is unique and which is associated at the endpoint with a security association or SA. Col. 21, lines 58-67. Encapsulation is performed in transport mode by encapsulating upper

layer protocol information in an ESP header and trailer and retaining an original IP 48 header and encapsulating an entire IP packet. Col. 23, lines 46 -58. See Figure 18. Encapsulation is used in tunnel mode as shown in Figure 18 for packets 270 and 272. A tunnel IP header encapsulates an AH or ESP header which encapsulates the original IP packet which encapsulates the TCP or UDP header. The combination of the unique IP address in the original IP1 header and the unique port number in the TCP or UDP header (obtained using PAP) defines a unique identity for any device or process on the LAN that needs secure communication. An SA can be bound to this unique identity so the authentication and encryption services of the AH and ESP protocols can be practiced. DNAT is used by devices on the LAN to request locally unique security values per the flowchart of Figure 19. Encapsulating this whole secure packet structure in a tunnel IP packet allows the IPsec packet to transition subsequent NATs without violating IPsec parameters. One could look at this the other way around and say that the TCP header is used to encapsulate the IPsec packet structure so one might assume at first blush that the Examiner is right about this anticipation rejection.

The applicants respectfully disagree. What Nessett does not teach is the step of determining if the encapsulation is necessary before actually doing it. In other words, IPsec packets can transition across a data path from the first computer device to the second computer device without encapsulation in TCP or UDP packets if they do not encounter NAT or protocol conversions. In such a case, the extra computational burden of doing encapsulation of an IPsec tunnel packet in a TCP or UDP packet is not necessary. Nessett assumes that NAT will be encountered and encapsulates the IPsec packet structures in tunnel IP packets (or TCP headers depending upon how one looks at Figure 18) without first determining if such encapsulation is necessary. If it is not necessary and Nessett does it anyway, which Nessett appears to teach, then

computational resources are wasted.

The invention includes as its first step a discovery process to determine if NAT or protocol conversions are occurring which make encapsulation in a TCP packet necessary. This is discussed at page 21 of the specification starting at line 4, and is done by sending the IP addresses a receiving node sees in the receiving node's Phase 2 Quick Mode messages as private payloads. These IP addresses can be compared by the first node to the IP addresses it put in the packets transmitted to the second node to determine if they are different. If they are different, that is an indication that NAT has occurred and that encapsulation is necessary in order to do IPsec. If no NAT or protocol conversion occurred, then encapsulation of IPsec packets in TCP headers is not necessary. The first step of claim 1, as amended herein, is:

> - determining what network address translations and/or protocol conversions, if any, occur on packets transmitted in a data path between said ~~the~~ first computer device and ~~the~~ said second computer device on packets transmitted between said first computer device and said second computer device,

This step should be interpreted in accordance with the teachings of the specification at page 21 and 22 and equivalent processes. Two different specific ways of doing this are taught in pages 21 and 22. One way of determining whether NAT or protocol conversions occurred is by sending as private payload sections of IKE Phase 2 Quick Mode messages the IP addresses seen by the sending node for the initiator and the responder, as shown in Figure 2b. Another way is by examining the port numbers of the received packets against the standard IKE port number 500. If the port number has changed, a translation has occurred. Page 22, lines 14 -17.

Because claim 1 has this discovery process as its first step, and because Nessett does not teach such a discovery process, claim 1 does not have all its elements taught in Nessett and is not anticipated. Since claims 2-7 all depend from claim 1, they

are not anticipated.

Claim 8 contains the process step:

> finding out, whether or not said second computer device supports a communication method where:
>
> it is determined what network address translations or ~~and/or~~ protocol conversions or both, if any, occur on packets transmitted between said first computer device and said second computer device;

This step should be interpreted like the first process step of claim 1 and in accordance with the teachings in the specification at pages 21 and 22 regarding how discovery of the existence of NAT and/or protocol conversions on the data path between the first and second computer devices is carried out and equivalent processes. Because Nessett does not teach a discovery process to determine if NAT or protocol conversions are occurring on the data path between the first and second computer devices, claim 8 is not anticipated.

Note that in both claim 1 and claim 8, the encapsulation of packets conforming to a first secure protocol that is incompatible with NAT or protocol conversions is conditional, *i.e.,* it is only done in response to the determination by the first discovery step that such NAT or protocol conversions are occurring on the data path between the first and second computer devices. If a determination is made that no NAT or protocol conversions are occurring, then no encapsulation is necessary and no encapsulation is done, thereby saving computing resources. Nessett does not teach the discovery process or a conditional encapsulation based upon the results of the discovery process.

New claim 24 includes this discovery process as its first step and is similar to claim 1 but has had the decapsulating step removed so as to focus upon only what happens at the first computer device and not include any steps that happen at the second computer device so as to simplify any infringement case. New claim 26 depends from new claim 24 and specifies the details of one embodiment for performing the

discovery process using Phase 2 Quick Mode messages which include IP addresses in the private payload sections and includes a step to compare these IP addresses to the IP address in the packet headers. If there is a difference, then a NAT or protocol conversion has occurred on the data path between the first computer device and the second computer device. New claim 27 adds the step of periodically transmitting keepalive packets at an interval set to make sure the NAT mapping or protocol conversion mapping tables do not change. Nessett does not teach keepalive packet transmission for this purpose or for any purpose.

New claim 25 depends from claim 24 and adds a step for negotiation before the discovery process to determine if the second computer device supports a secure data communication protocol. New claim 27 depends from new claim 24 and specifies the discovery process as comparing the port numbers of the received packet to the IKE port number of 500 to determine if port translations occurred.

New claim 29 focusses solely on what the second computer does.

New claim 30 is an independent claim that has had the steps regarding operations by the second computing device removed and which includes the steps of claim 1 and additional steps such as: 1) doing a negotiation with the second computer to determine if it supports a secure protocol before doing the discovery process to determine if any NAT or protocol conversions are happening on the data path; 2) periodically transmitting keepalive packets if NATs are occurring so as to keep the NAT mapping tables fixed. Nessett does not teach this combination of steps. New claims 31-33 depend from claim 30 and add various details such as how the discovery process is performed.

Allowance is respectfully requested, and the undersigned respectfully requests a telephonic interview.

Respectfully submitted,

Dated: October 6, 2004

Ronald Craig Fish
Reg. No. 28,843
Tel 408 778 3624
FAX 408 776 0426

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail, postage prepaid, in an envelope addressed to: Commissioner for Patents , P.O. Box 1450, Alexandria, Va. 22313-1450.
on 10/6/2004
(Date of Deposit)

Ronald Craig Fish, President
Ronald Craig Fish, a Law Corporation
Reg. No. 28,843